ATNP/WG2/WP.....
10 July 2000

AERONAUTICAL TELECOMMUNICATION NETWORK PANEL

Working Group 2

21st Meeting

Limerick, Ireland

11 – 14 July 2000

SME 5 (Internet Communications Service) Status Report

Working Paper

Presented by Klaus-Peter Graf (Sub-Volume 5 SME)

Summary

This paper provides a summary report on the status of the PDRs which have been submitted against the ATN ICS SARPs (Sub-Volume 5 of Doc 9705) since ATNP/3 and other CCB-related matters.

Furthermore it presents the proposed solution of PDR M0040002 for review by the meeting.

1 Introduction

This paper provides a summary on the status of the Proposed Defect Reports (PDRs) raised against the ATN Internet Communications Service (ICS) SARPs since ATNP/3 in February 2000 for information of the WG2 members.

Furthermore it presents 14 PDRs which have been raised against Draft Edition 3 of the ICS SARPs as a result of validation activities on enhancements made in Draft Edition 3. These PDRs have been labelled as "P3DRs" and distributed on the WG2_SDM mailing list for discussion and resolution. They have also been reviewed by IDG/4 in April 2000 and most of them have been resolved and appropriate corrective actions made to Draft Edition 3 of the ICS SARPs.

1 PDR Status

Table 1 presents the list of those PDRs which have been submitted to the ATNP Configuration Control Board (CCB) since its last meeting in December 1999 and which apply to the Internet Communications Service (ICS) SARPs.

It should be noted that this table only contains PDRs raised against Edition 1 and/or Edition 2 of the ICS SARPs as Draft Edition 3 is not yet under configuration control by the ATNP CCB and consequently no CCB-controlled defect resolution mechanism is available for this last edition up to now.

PDR Number	PDR Title	CCB Status	SDM Status
M0040001	Incorrect/Duplicated ATSC Class Security Tag Requirement	PROPOSED	RESOLVED
M0040002	Extended Transport Checksum	PROPOSED	RESOLVED

Table 1: Status of ICS PDRs in the ATNP CCB Process

Whereas the resolution for PDR M0040001 is straightforward, PDR M0040002 is attached to this paper as Appendix A for review and approval by WG 2 members. Appendix B contains a comment received on this PDR for consideration by the meeting.

1 Potential Draft Edition 3 Defects

As a result of comprehensive validation exercises performed by STNA, the following potential defects have been identified in Draft Edition 3 of the ICS SARPs since the last WG2 meeting in December 1999. These potential defects relate to enhancements introduced in Draft Edition 3 and have no impact on Editions 1 and 2 of the ICS SARPs. Resolution of these potential defects is not under control by the CCB, but within the responsibility of the WG2 SDM process. These PDRs have been registered by the SME 5 in the form of P3DRs and distributed on the WG2_SDM mailing list for discussion and resolution.

P3DR Number	P3DR Title	SDM Status	Resolved in Draft Edition 3
M0020010	Processing of received Deflate Maintenance Parameter	RESOLVED	Yes
M0020011	Issues on the concept of Subnetwork Connection Group	RESOLVED	Yes

M0020012	Bit 0 of the ISH Data Link Capability Parameter	RESOLVED	Yes
M0020013	TP4 retransmission timer on the first RTT sample	RESOLVED	Yes
M0020014	Valid/invalid round trip time sample in TP4	RESOLVED	Yes
M0020015	Error condition for Deflate decompressor window	SUBMITTED	
M0020016	Use of received security info by Airborne BIS	RESOLVED	Yes
M0020017	Interoperability problem due to the suppression of ACA	RESOLVED	Yes
M0020018	Interoperability with a peer BIS that does not support authentication type 2	SUBMITTED	
M0020019	BIS behaviour in case of certificate path validation failure	RESOLVED	Yes
M0020020	A/G BIS access to delivery service	RESOLVED	No (GM)
M0020021	Encoding of Random Variable Parameter value	RESOLVED	Yes
M0020022	Length of Certificate Path Parameter	RESOLVED	Yes
M0020023	Alignment of Reset Request and Reset Indication Procedures	SUBMITTED	

Table 2: Identified Defects in Draft Edition 3 of the ICS SARPs

All of the above defects are classified as minor/clarification, i.e. no major deficiency has been identified on the ICS enhancements so far.

1 Recommendation

The meeting is invited to

- note the above reported status; and
- review and approve the proposed solution for PDR M0040002 attached to this report.

Appendix A

Title:	Potential Misdelivery of CLNP Packets
PDR Reference:	M0040002
Originator Reference:	
SARPs Document Reference:	ICS SARPs, Section 5.5.2.4
Status:	ACCEPTED
Impact:	A (Critical)
PDR Revision Date:	SUBMITTED → ACCEPTED(23/5/00) ACCEPTED → PROPOSED (26/6/00)
PDR Submission Date:	13/04/00
Submitting State/Organisation:	Eurocontrol
Submitting Author Name:	Tony Whyman
Submitting Author E-mail Address:	tony.whyman@fans-is.com
Submitting Author Supplemental Contact Information:	
SARPs Date:	SV 5 Edition 2
SARPs Language:	English

Summary of Defect:

In ICAO Doc 9705 Subvolume one, it is required that:
"1.3.28 The end system shall make provisions to ensure that the probability of not detecting a 255-octet message being mis-delivered, non-delivered or corrupted by the internet communications service is less than or equal to 10-8 per message."

Currently there is no ensurance that this requirement is met by systems which implement the technical provisions of the ATN SARPs.
It seems that validation of this SV1 requirement has not been done to a level which clearly indicates that the risk of either mis-delivery of CLNP packets by the ATN ICS or not detecting mis-delivered packets is less than or equal to 10-8.

There are at least three possible methods of resolution:
a) Further validation material is submitted which indicates that the possibility of mis-delivery or non-detection of mis-delivered packets is less than 10-8.
b) Additional measures are taken in the ATN applications to ensure that mis-delivered messages are detected and not operated upon.
c) Additional measures are added to the ATN ICS to ensure that mis-directed CLNP packets are discarded by the receiver and packet recovery mechanisms are initiated.

The discussion part of this PDR and the proposed SARPs amendement

below relate to the third option. The presented solution is favoured by the IDG in the case that resolution if this PDR is aimed at the ICS level. However, it is not intended to exclude any proposals for resolution falling into category a) or b) above.

Discussion:

If a TPDU is mis-delivered to the wrong destination then this can be detected through:
a) an incorrect Destination NSAP Address in the CLNP header;

b) an inconsistency in the TPDU header information; or
c) an inconsistency in the application data.
Unfortunately, it is not possible to rely upon any of the above to detect mis-delivery to the required level.

The ATN ICS SARPs currently do not include a genuine end-to-end check on the integrity of the CLNP Destination NSAP Address; the CLNP Header Checksum is not an end-to-end checksum as it is manipulated by intermediate systems and is anyway discarded by LREF. However, it is possible to extend the transport checksum to include the destination NSAP Address without having to include

the NSAP Address itself in the transport protocol header. This will provide an end-to-end check on NSAP Address integrity and hence provide the receiving transport entity with a means of detecting and rejecting TPDU mis-delivered due to an undetected error in the destination NSAP Address or an LREF problem.

A means to achieve this may be found in TCP. The TCP/IP world has traditionally been less concerned with layer independence than the OSI world and the TCP checksum includes the source and destination IP addresses within its scope by constructing a “pseudo header” including these fields. This pseudo header is never transmitted but is assumed to the part of the TCP header for checksum computation purposes. When a packet is received, the receiving system reconstructs the pseudo header from the information contained in the IP header and verifies the checksum and hence IP Address integrity.

An extended transport checksum could readily be defined for TP4 to include the source and destination NSAP Addresses in a similar pseudo header or trailer. This may then be used to detect mis-delivery and hence avoid the identified hazards.

However, in order to meet the requirement for better than 1 in 10E8 such errors to remain undetected, a better checksum algorithm is also required. This is because the existing 16 bit checksum has an undetected error rate of the order of 1 in 10E5. A 32-bit ones complement checksum will have an undetected error rate of the order of 1 in 10E10 and hence this is preferred for an extended checksum.

Proposed SARPs Amendment:

1) Add the following new para 5.5.2.2.15 and subsequent sub-paras:

"5.5.2.2.15 Negotiation of the Use of the Extended Transport Checksum

5.5.2.2.15.1 When supported, the use of the Extended Transport Checksum shall be proposed by an ATN End System during connection establishment by including an Extended Transport Checksum parameter in a CR TPDU as specified in 5.5.2.4.3.

Note.- The ISO/IEC 8073 checksum parameter is also included in the CR TPDU in order to comply with the ISO/IEC standard and to support backwards compatibility.

5.5.2.2.15.2 The use of the 16-bit checksum shall be proposed in the ”Additional Option Selection” parameter of the CR TPDU.

5.5.2.2.15.3 When a CR TPDU is received that includes the Extended Transport Checksum parameter, then the connection responder shall

a) include an Extended Transport Checksum parameter, as specified in 5.5.2.4.3, in the responding CC TPDU;

Note.- The connection responder may select the 2-octet long or 4-octet long Extended Transport Checksum parameter in the responding CC TPDU.

b) ommit the ISO/IEC 8073 checksum parameter from the responding CC TPDU;

c) reject the use of the 16-bit checksum in the ”Additional Option Selection” parameter of the responding CC TPDU.

5.5.2.2.15.4 All other TPDUs exchanged on the same transport connection shall also include the Extended Transport Checksum parameter with the same length as selected in the CC TPDU and shall not include the ISO/IEC 8073 checksum parameter.

5.5.2.2.15.5 A CR TPDU that does not contain an Extended Transport Checksum parameter shall be processed in compliance with ISO/IEC 8073.

5.5.2.2.15.6 If a CR TPDU without an Extended Transport Checksum parameter is received, then an Extended Transport Checksum parameter shall not be included in any TPDUs sent on that transport connection.

5.5.2.2.15.7 If a CC TPDU is received that includes an Extended Transport Checksum parameter, then all other TPDUs exchanged on the same transport connection shall

a) also include the Extended Transport Checksum parameter with the same length as specified in the CC TPDU,and

b) not include the ISO/IEC 8073 checksum parameter.

5.5.2.2.15.8 If a CC TPDU is received that does not include an Extended Transport Checksum parameter, then

a) the CC TPDU shall be processed in compliance with ISO/IEC 8073, and

b) an Extended Transport Checksum parameter shall not be included in any TPDUs sent on the transport connection.

5.5.2.2.15.9 If both an Extended Transport Checksum parameter and either the ISO/IEC 8073 checksum parameter are present, or 16-bit checksums are accepted by the connection responder, or both, then this shall be treated as a protocol error."

2) Add the following new para 5.5.2.4.3 and subsequent sub-paras:

"5.5.2.4.3 Encoding of the Extended Transport Checksum Parameter

5.5.2.4.3.1 The Extended Transport Checksum Parameter shall be

encoded as a variable part TPDU parameter using one of the two following formats:

Parameter Code: 0000 1000,indicating Extended Transport Checksum parameter with 4 octets length
Parameter Length: 4
Parameter Value: Result of the checksum algorithm as specified in 5.5.2.7.3.4

or

Parameter Code: 0000 1001,indicating Extended Transport Checksum parameter with 2 octets length
Parameter Length: 2
Parameter Value: Result of the checksum algorithm as specified in 5.5.2.7.3.3

Note.— When supported, the parameter is included in a CR TPDU and is thereafter included in all other TPDUs except when the connection responder indicates non-support of the parameter by omitting it from the variable part of the CC TPDU.

5.5.2.4.3.2 An Extended Transport Checksum parameter shall only be used when both connection initiator and receiver have been assigned NSAP Addresses in the ATN Network Addressing Subdomain.

5.5.2.4.3.3 An Extended Transport Checksum Parameter received in a TPDU other than a CR TPDU and from a source NSAP with an NSAP Address in any other Addressing Subdomain shall be treated as a protocol error; in a CR TPDU it shall be ignored.

Note 1.— Use of this parameter is not in compliance with ISO/IEC

8073. However, it is not a protocol error to use it in a CR TPDU. Hence,as long as it is only used when both initiator and receiver indicate support by including it in the CR TPDU, and in a CC TPDU in response to such a CR TPDU, its implementation will not result in interoperability problems.

Note 2.— Parameter codes with bits 7 and 8 are explicitly not assigned by ISO/IEC 8073, nor is their use precluded.

Note 3.— Requiring that both sender and receiver are ATN Systems

ensures that the correct semantics of the parameter are observed.

5.5.2.4.3.4 In a CR TPDU, the Extended Transport Checksum shall be calculated first and the resulting check digits inserted into the TPDU before the 16-bit checksum is calculated.

5.5.2.4.3.5 The value of the 16-bit checksum parameter shall be set to zero before the Extended Transport Checksum is computed.

5.5.2.4.3.6 When present in a TPDU, the Extended Transport Checksum parameter shall be validated using the algorithm specified in 5.5.2.7.

5.5.2.4.3.7 If the validation fails, the TPDU shall be discarded without further processing.

5.5.2.4.3.8 When a CR TPDU is received, the 16-bit checksum shall be verified as correct before the Extended Transport

Checksum is verified."

3) Add the following new para 5.5.2.7 and subsequent sub-paras:

"5.5.2.7 Extended Transport Checksum Computation

Note.— The style of Appendix B of ISO/IEC 8073 is followed in the definition of the extended transport checksum algorithm.

5.5.2.7.1 Symbols

Note.- The following symbols are used:

a) C0, C1, C2, C3 are variables used by the algorithm
b) i is the number (i.e. position) of an octet within the TPDU
c) n is the number (i.e. position) of the first octet of the Extended Transport Checksum parameter
d) L is the length of the complete TPDU including the "pseudo trailer"
e) Xj is the value of the jth octet of the Extended Transport Checksum parameter (in transmission order).

5.5.2.7.2 Arithmetic Conventions

5.5.2.7.2.1 Addition shall be performed in one of the two following modes:

a) modulo 255
b) ones complement arithmetic in which if any of the variables

has the value minus zero (i.e. 0xFFFF) shall be regarded as though it were plus zero (i.e. 0).

5.5.2.7.3 Algorithm for Generating the Checksum Parameters

5.5.2.7.3.1 The complete TPDU with the Extended Transport Checksum Parameter value field set to zero shall be set up.

5.5.2.7.3.2 A "pseudo trailer" created from:
a) the length of the destination NSAP Address
b) the destination NSAP Address
c) the length of the source NSAP Address
d) the source NSAP Address,
encoded identically to their encoding in the CLNP header shall be appended to the TPDU.

Note 1.— This pseudo trailer is not part of the TPDU and is never transmitted to the destination end system.

Note 2.— A pseudo trailer rather than a pseudo header is used because the check digits have to be moved to the end of the TPDU by the receiver and hence a trailer will have to be constructed anyway.

5.5.2.7.3.3 The 2-octet long Extended Transport Checksum shall be created by the following algorithm:

1) Initialise C0 and C1 to zero

2) Process each octet in the combined TPDU and pseudo trailer sequentially from i = 1 to L by

a) adding the value of the octet to C0; then
b) adding the value of C0 to C1.

3) Set the octets of the Extended Transport Checksum parameter as follows:
a) X0 = -C1 + (L-n)*C0
b) X1 = C1 - (L-n+1)*C0.

4) Discard the pseudo trailer octets.

5.5.2.7.3.4 The 4-octet long Extended Transport Checksum shall be created by the following algorithm:

1) Initialise C0 , C1, C2 and C3 to zero

2) Process each octet in the combined TPDU and pseudo trailer sequentially from i = 1 to L by
a) adding the value of the octet to C0; then
b) adding the value of C0 to C1, C1 to C2, and C2 to C3

3) Set the octets of the Extended Transport Checksum parameter as follows:
a) X0 = - (C0 + C1 + C2 + C3)
b) X1 = C1 + 2*C2 + 3*C3
c) X2 = - (C2 + 3*C3)
d) X3 = C3

4) Discard the pseudo trailer octets.

5.5.2.7.4 Algorithm for Checking the Checksum Parameters

5.5.2.7.4.1 The transport entity shall appended to the received TPDU a "pseudo trailer" which is created from the source and destination NSAP Addresses associated with the incoming TPDU and the value of the received Extended Transport Checksum parameter in the following order:
a) the length of the destination NSAP Address
b) the destination NSAP Address
c) the length of the source NSAP Address
d) the source NSAP Address,
encoded identically to their encoding in the CLNP Header,
e) the octets of the Extended Transport Checksum parameter in the same order in which they appear in the checksum parameter.

5.5.2.7.4.2 The value of the Extended Transport Checksum Parameter shall be set to zero.

5.5.2.7.4.3 If the received TPDU is a CR TPDU, then the value of the 16-bit checksum parameter shall be set to zero.

5.5.2.7.4.4 If the received TPDU contains a 4-octet long Extended Transport Checksum, this checksum shall be validated as follows:

1) Initialise C0, C1, C2 and C3 to zero

2) Process each octet in the combined TPDU and pseudo trailer sequentially from i = 1 to L by
a) adding the value of the octet to C0; then
b) adding the value of C0 to C1, C1 to C2, and C2 to C3

3) Discard the pseudo trailer.

4) If, when all the octets have been processed, one or more of the variables C0, C1, C2 or C3 do not have the value zero,then the checksum validation has failed.

5.5.2.7.4.5 If the received TPDU contains a 2-octet long Extended

Transport Checksum, this checksum shall be validated as follows:

1) Initialise C0 and C1 to zero

2) Process each octet in the combined TPDU and pseudo trailer sequentially from i = 1 to L by
a) adding the value of the octet to C0; then
b) adding the value of C0 to C1

3) Discard the pseudo trailer.

4) If, when all the octets have been processed, one or more of the variables C0 and C1do not have the value zero, then the checksum validation has failed."

5) Add the following new APRL item to para 5.5.2.8.1.2.2:

"ATN7 Use of Extended Transport Checksum 5.5.2.2.15.1, 5.5.2.4.3.2 O"

6) Add the following new para 5.5.2.8.1.13:

"5.5.2.8.1.13 Extended Transport Checksum

ETC1 Extended Transport Checksum in CR TPDU 5.5.2.2.15.1 ATN7:M
ETC2 Proposal of 16-bit Checksum in CR TPDU 5.5.2.2.15.2 ATN7:M
ETC3 Extended Transport Checksum in CC TPDU 5.5.2.2.15.3 ETC1:M
ETC4 ISO/IEC 8073 Checksum Parameter in CC TPDU 5.5.2.2.15.3 ETC1:X
ETC5 Rejection of Use of 16-bit Checksum in CC TPDU 5.5.2.2.15.3 ETC1:M
ETC6 Extended Transport Checksum all subsequent TPDUs 5.5.2.2.15.4, 5.5.2.2.15.6, 5.5.2.2.15.7, 5.5.2.2.15.8 (ETC1 and ETC3):M
ETC7 Encoding of Extended Transport Checksum 5.5.2.4.3 ATN7:M
ETC8 Computation of Extended Transport Checksum 5.5.2.7.3 ATN7:M
ETC9 Validation of Extended Transport Checksum 5.5.2.7.4 ATN7:M"

7) Add the following new para 5.5.3.4.2:

"5.5.3.4.2 Extended Transport Checksum

5.5.3.4.2.1 An Extended Transport Checksum parameter shall be included in the varible part of an UD TPDU when both the sending and receiving end system have been assigned NSAP addresses in the ATN Network Addressing Subdomain.

Note 1.— Requiring that both sender and receiver are ATN Systems ensures that the correct semantics of the parameter are observed.

Note 2.- The ISO/IEC 8602 16-bit checksum parameter may also be included in the UD TPDU.

5.5.3.4.2.2 The Extended Transport Checksum parameter shall be encoded as follows:

Parameter Code: 0000 1000
Parameter Length: 4
Parameter Value: Result of the algorithm for the 4-octets long Extended Transport Checksum as specified in 5.5.2.7.3

Note 1.— Use of this parameter is not in compliance with ISO/IEC 8602. However, as long as it is only used by communicating ATN End Systems,its implementation will not result in interoperability problems.

Note 2.— Parameter codes with bits 7 and 8 set to zero are explicitly not assigned by ISO/IEC 8602, nor is their use precluded.

5.5.3.4.2.3 If both the Extended Transport Checksum parameter and the ISO/IEC 8602 16-bit checksum parameter are present in an UD TPDU, then the Extended Transport Checksum shall be calculated first and the resulting check digits inserted into the UD TPDU before the 16-bit checksum is calculated.

5.5.3.4.2.4 An UD TPDU that does not contain an Extended Transport Checksum parameter shall be processed in compliance with ISO/IEC 8602.

5.5.3.4.2.5 When present in a received UD TPDU, the Extended Transport Checksum parameter shall be validated using the algorithm for the 4-octets long Extended Transport Checksum parameter as specified in 5.5.2.7.4.

5.5.3.4.2.6 When the validation fails, the TPDU shall be discarded without further processing."

8) In the APRL table of para 5.5.3.6.2 modify the entry in line 7 as follows:

"TpTc <t> TPDU UD Checksum 6.2.4.1 O O"

9) Add the following new APRL items to para 5.5.3.6.2:

"TpTetc <t> TPDU UD Extended Transport Checksum 5.5.3.4.2 (ATN SARPs) -- M"

"TpRetc <r> TPDU UD Extended Transport Checksum 5.5.3.4.2 (ATN SARPs) -- M"

Impact on Interoperability:

The solution proposed for the COTP is backwards compatible, as the

use of the Extended Transport Checksum is negotiated during connection establishment. The additional checksum is not included in subsequent TPDUs if the negotiation reveals that one of the communicating entities does not support this feature.
The solution proposed for the CLTP is not backwards compatible and there is no way to introduce this feature in a way that ensures interoperability with previous editions. Therefore, the impact category of this PDR has been upgraded to category A (Critical). However, it is assumed that there is no operational system implementing the Edition 1&2 short stack CLTP and consequently the impact on existing implementations should be minimal.

SME Recommendation to CCB: Accept proposed SARPs Amendment

CCB Decision: PDR Accepted (23/05/99)

Appendix B

RE: P1DR M0040002 PROPOSED
Date: Mon, 3 Jul 2000 11:40:26 +0100
From: "Fieldhouse, Dirk" <Fieldhouse@logica.com>
To: "'ATNP WG/2 Mailing List'" <atnp_wg2@tls.cena.fr>

All,

Sorry to be a layer pedant, but assuming for the moment that there is a need for an extended checksum as proposed below, should it not be a CLNP option (say, "CLNP extended checksum")? Although the local NSAP address is a mandatory parameter of the CLNS N-UNITDATA.req primitive, there may be implementations that do not make the local NSAP address explicitly available when a TPDU is being constructed. With any luck these do not include any extant ATN CLNP/TP4 implementations.

Note that IP6 has a clear concept of end-end options vs hop-by-hop options, or did when I last checked.

It would then be necessary to consider:

- should the transport checksum option, when selected, be suppressed if the CLNP extended checksum is selected, and if so how?

- how would this CLNP extended checksum option interact with LREF compression (in particular, be preserved end-to-end without disabling the use of LREF)?

- would it only be carried in the initial NPDU in case of fragmentation?

/df